Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Policies and Rules Concerning Toll Fraud	)	CC Docket No. 93-292
	)	

COMMENTS OF SPRINT CORPORATION

Jay C. Keithley
Michael B. Fingerhut
Norina T. Moy
1850 M St., N.W., Suite 1110
Washington, D.C. 20036
(202) 857-1030

Craig T. Smith
P.O. Box 11315
Kansas City, MO. 64112
(913) 624-3065

January 14, 1994

TABLE OF CONTENTS

Summary

Sprint Corp. actively supports additional efforts to develop effective and efficient measures to avoid or reduce the risks of toll fraud. To that end, Sprint Long Distance has implemented aggressive toll fraud customer education and monitoring programs; has tariffed a toll fraud insurance offering (SprintGuard Plus); and has included tariff language which points out the possibility that toll fraud may occur and that the customer may be responsible for toll fraud charges. United Telephone has tariffed several blocking and screening services, as well as LIDB service, and has implemented a sales program which includes the provision of information on toll fraud to the customer. Sprint Cellular has implemented pre-call or post-call validation mechanisms, and is developing more advanced fraud control systems using, among other things, analysis of radio transmission characteristics and voice recognition technology.

Sprint endorses the general principle that determination of toll fraud liability should reflect each party's relative ability to prevent and detect fraud, and its affiliated carriers have integrated such principle in their business operations. (Sprint would point out, however, that some instances of fraud will occur even if all the parties involved make every reasonable effort to prevent such fraud. Furthermore, the IXC and the LEC cannot always positively identify fraud; they can only detect unusual traffic patterns. It is ultimately the responsibility of the customer to determine

whether anomalous calling activity is legitimate or fraudulent.) Adoption of this general principle, rather than specific rules or formulas which attempt to assess liability, should be sufficient to protect the interests of affected parties. Should this general principle prove to be unworkable or insufficient, the Commission could consider more detailed rules at a future date.

There are a number of measures which can be taken to reduce the risk of payphone and cellular toll fraud, including installation of equipment or software which identifies a line as a payphone; use of the 8000 and 9000 numbering scheme for payphones; transmission by cellular carriers of relevant information digits in the call detail record which identifies cellular calls; implementation of pre-call verification procedures for all cellular calls; and adoption of a Part 22 rule which requires cellular phone design which prohibits transmission of anything other than the original factory-installed ESN.

Similarly, fraud related to alternative billing services (calling card, collect, and billed to third party calls) can be reduced through measures such as commitment by LIDB providers to specific LIDB operational standards for fraud trigger thresholds, handling of customer fraud referrals, normal and emergency updates, etc.; provision and use of "called from" and "called to" numbers; and improved coordination between LEC data owners and LIDB providers.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

DOCKET FILE COPY ORIGINAL

In the Matter of	)	
	)	
Policies and Rules Concerning Toll Fraud	)	CC Docket No. 93-292
	)	

COMMENTS

Sprint Corporation ("Sprint"), on behalf of Sprint Communications Company LP ("Sprint Long Distance"), the United and Central Telephone Companies ("United Telephone"), and Sprint Cellular, hereby respectfully submits its comments in the above-captioned notice of proposed rulemaking (NPRM).

In the instant NPRM, the Commission seeks comment on proposals to achieve closer coordination between the entities fighting toll fraud; improve consumer education initiatives; assess the reasonableness of tariff liability provisions; establish a federal policy assigning liability for telephone fraud; codify a requirement for written warnings for telecommunications equipment registered under Part 68 of the Rules; and determine measures to prevent CPE, cellular and line information database (LIDB) fraud. As discussed below, Sprint actively supports additional efforts to develop effective and efficient measures to avoid or reduce the risks of toll fraud. Many of the proposals set forth in the NPRM have substantial merit, and their implementation should be strongly encouraged, but not necessarily mandated, by the Commission.

I. COORDINATION AND CUSTOMER EDUCATION MEASURES SHOULD BE STRONGLY ENCOURAGED.

As the Commission recognizes in the NPRM (para. 11), toll fraud is a serious problem involving many different entities, including the customer, carriers (local, interexchange, cellular and reseller), validation service providers, equipment vendors, and regulatory and law enforcement agencies. Because of the costs imposed by toll fraud on Sprint and its customers, Sprint fully supports efforts to improve coordination among these parties to prevent, detect and prosecute toll fraud crimes.

Sprint therefore welcomes efforts by the Commission to help persuade the Congress to enact more specific legislation to penalize toll fraud perpetrators and to give law enforcement agencies the tools they need to track and prosecute such perpetrators. Even a relatively simple change such as amending existing statutes (e.g., 18 U.S.C. Section 1029, the Access Device Fraud statute) to specifically reference telecommunications toll fraud would help to clarify the applicability of such laws to telephone fraud crimes.

Sprint also agrees that "closer and continuing coordination among the institutions fighting toll fraud" (NPRM, para. 13) can be facilitated through a broad-based organization dedicated to addressing toll fraud issues. At least two such organizations already exist--the Communications Fraud Control Association (CFCA), and the Toll Fraud Prevention Committee (TFPC) of the Network Operations Forum. Participation in the CFCA is open to all interested parties, and representatives of

regulatory and law enforcement agencies, carriers, and vendors participate in the TFPC (with some change in the by-laws, participation in the TFPC by end user customers could no doubt also be arranged).[1] Coordination of toll fraud prevention measures will be facilitated if such efforts are consolidated within a single or dual venue rather than spread across several different organizations.

Sprint also firmly supports efforts to heighten awareness of the risks of toll fraud and the ways to minimize such risks. To that end, Sprint's local, long distance and cellular divisions have each implemented aggressive programs to combat toll fraud, including many of the toll fraud prevention measures cited in the NPRM. For example, Sprint's long distance subsidiary offers the following services to its customers:

- Sprint monitors and analyzes traffic patterns (for services such as domestic 800; inbound international toll free; outbound international, including area code 809; calling card (Sprint FONcards as well as LEC and bank calling cards); collect; billed-to-third party; and cellular traffic) for unusual calling patterns, notifies the customer of any abnormal activity, and will recommend corrective action. Sprint's calling card monitoring systems are connected directly to databases which provide validation and call detail information. A compromised

---

[1] Assuming that participation in the TFPC can be broadened to include companies and regulatory and law enforcement agencies who currently do not participate in the TFPC, establishment of a new "Federal Advisory Committee" (NPRM, para. 13) would seem unnecessary. It would appear that the CFCA and an expanded TFPC could fulfill most (if not all) of the functions envisioned by the Commission for its Federal Advisory Committee.

card or ANI can be disabled with a single keystroke.

- Sprint corporate security personnel provide educational and consultative services (e.g., to instruct customers on how to protect their CPE against fraud, to identify system vulnerabilities, to recommend effective preventive measures, etc.); assist in toll fraud investigations and provide appropriate security support; and can act as the interface between the customer and appropriate law enforcement agencies as well as with other domestic and international carriers. Sprint security personnel also monitor electronic bulletin boards to identify compromised codes and unauthorized system access methods, and actively participate in fora dealing with toll fraud issues.

- Sprint offers SprintGuard Plus (TM), a tariffed service offering which limits the subscriber's financial loss while providing specialized security support services, including CPE-related abnormal activity call detail reports and periodic bulletins about CPE fraud and prevention methods.

- In addition to presentations by Sprint sales and security personnel, written information about SprintGuard Plus, SprintGuard CPE Security Support Services, and calling card fraud is distributed to current and potential customers (see, for example, the brochures included as Attachment A).

Sprint's local telephone companies have also implemented several measures to prevent toll fraud, including:

- Provision of originating line screening (OLS), billed number screening (BNS), and Toll Restriction (TR) (which blocks all 1+ calls) services;[2]

---

[2]Except for the states listed below, OLS and BNS services are 100% available in all of United and Centel's jurisdictions. For these exception states, the availability ratios are as follows:

(Footnote Continued)

- Provision of international toll blocking service;

- Implementation of a line information database (LIDB), which is manned 365 days a year;

- Inclusion in sales and marketing programs of customer information about toll fraud (see, e.g., "Business Telephone System Security" brochure, included as Attachment B).

Sprint Cellular has implemented either pre-call or post-call validation systems for all of its cellular traffic. (Post-call validation systems check the status of a roaming customer after placement of an initial call. If the phone is identified as invalid, an entry is placed in a "negative file" and no further calls are allowed.) Sprint Cellular is also developing more advanced fraud control systems using recognition of fraudulent calling patterns, analysis of radio transmission characteristics, voice recognition, complex validation algorithms, and other methods to help combat cellular cloning.

As is clear from the toll fraud prevention services described above, Sprint has already taken aggressive steps "to ensure that these warnings [of risk of fraud from using the carrier's services] are communicated effectively to customers..."

(Footnote Continued)

	OLS	BNS
Indiana	94%	100%
Missouri	34%	100%
North Carolina-United	71%	100%
North Carolina-Centel	78%	100%
Ohio	65%	100%
Pennsylvania	84%	84%
South Carolina	97%	97%
Virginia-United	66%	97%
Virginia-Centel	85%	85%

(NPRM, para. 24). Because of the financial consequences resulting from toll fraud, and the need to maintain customer goodwill, carriers have a vested interest in the prevention and early detection of toll fraud involving their services, and Sprint therefore agrees that the Commission should emphasize a carrier's "affirmative duty" (id.) to warn its customers of the risks of toll fraud. However, rather than prescribing specific consumer education measures to be enacted by each carrier, Sprint believes that, in general, decisions on how to alert customers about the risks of toll fraud are best left to the carriers. Especially in markets where competition exists, marketplace pressures will force the carrier to offer security services and devices. Moreover, to the extent that service and equipment providers are required to accept some liability for toll fraud, such providers will have an additional financial incentive to ensure that their customers are aware of the possibility of toll fraud and of the available means of preventing or minimizing such fraud.[3]

---

[3]It is Sprint's impression that over the past couple of years, equipment (especially PBX) manufacturers have become increasingly active in educating their customers about the risks of CPE toll fraud. For example, most equipment manuals now appear to include warnings about the importance of changing factory-default codes, and default activation settings are now set to "off" rather than "on" (so that positive action is required to activate a feature). Given these improvements in equipment manufacturers' anti-fraud efforts, the proposed Part 68 rules would not seem to be necessary.

II. IN GENERAL, ASSESSMENT OF TOLL FRAUD LIABILITY SHOULD REFLECT THE DEGREE TO WHICH EACH PARTY CAN CONTROL SUCH FRAUD.

In the NPRM (para. 24), the Commission tentatively concludes that "tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of risks of using carrier services are unreasonable." The Commission's intent here is not entirely clear. If by this statement, the Commission is proposing that carriers' tariffs make clear that unauthorized calls might be charged to a customer's account, and that customers may be held responsible for such fraudulent calls, then Sprint has no objection to such proposal.[4] Indeed, Sprint Communication Company's current tariff language already warns subscribers of the possibility of toll fraud through (for example) their CPE, and their liability for such calls. This tariff states that Sprint:

> ...is not liable for any damages, including toll usage charges, the subscriber may incur as a result of the unauthorized use of its telephone facilities. This unauthorized use of the subscriber's facilities includes, but is not limited to, the placement of calls from the subscriber's premises, and the placement of calls through subscriber-provided equipment which are transmitted or carried on the Sprint network. The Sprint Corporate Security Department may work with subscribers to recommend possible solutions to reduce unauthorized use of their facilities. However, Sprint [Long Distance] does not warrant or guarantee that its recommendations will prevent all unauthorized use, and the subscriber is responsible for controlling access to, and use of, its own telephone facilities.

---

[4] If the Commission means otherwise, it should detail the type of language it believes should be added to carriers' tariffs and seek comment on such language.

See Sprint FCC Tariff No. 1, Section 3.4.6.[5]

The Commission further suggests (NPRM, para. 24) that the "dispositive element" in assessing liability for toll fraud should be "where responsibility for the detection and prevention of fraudulent calling" lies. Sprint endorses this principle, and its affiliated carriers have already incorporated it in their handling of toll fraud cases. For example, a Sprint Long Distance subscriber whose FONcard number was stolen, or a Sprint Cellular customer whose electronic serial number or mobile identification number was "tumbled" or cloned, are considered to have little control over such theft, and therefore are rarely, if ever, held liable for unauthorized toll calls. On the other hand, a customer who made little effort to control access to his CPE (e.g., did not disable the remote access feature, did not use unique personal identification numbers) is generally held liable for CPE-based toll fraud charges. Moreover, there are some situations in which the carrier should accept liability for toll fraud; for example, if an IXC decided to process a calling card call without first doing a database check to determine the validity

---

[5]In addition, customers who subscribe to SprintGuard Plus must comply with a number of requirements such as use of a minimum of 8 digits for each Direct Inward System Access code, and deletion of all CPE manufacturer/vendor-installed default passwords (see Sprint Tariff FCC No. 2, Section 4.6.17). Tariff provisions such as these heighten customers' awareness of the risks of toll fraud and of the steps they can take to minimize such risks.

of that card, then the IXC should be liable for any resulting fraud.

While Sprint does agree with the general principle that liability should accrue according to degree of control over the prevention of fraud, three other factors should be considered in making toll fraud liability determinations:

1. Any rule which attempts to identify which party is liable for toll fraud costs under different scenarios, and any formula which attempts to apportion liability, are likely to be unworkable. Because the list of toll fraud scenarios could be enormous, any attempt to catalogue the specific conditions under which various parties are liable will be incomplete, will inevitably lead to disputes, and will embroil the Commission in a series of proceedings to determine the extent of each party's culpability. Therefore, at least as a first step, the Commission should adopt only the general principle that liability should reflect ability to control the incidence of fraud. Customers who believe that they have been treated unfairly by their service provider in determining toll fraud liability would always have recourse to the Commission's complaint process as well as to other legal remedies. If adoption of this broad policy proves to be unworkable or insufficient, the Commission can consider more detailed rules for determining fraud liability at a future date.

2. It should be recognized that there will be some cases in which fraud occurs even if all the parties involved make every reasonable effort to prevent such fraud. For example, a payphone provider may experience toll fraud even if it

subscribes to OLS and BNS services; if the IXC performs the appropriate database lookup; and the database provider has maintained accurate and timely data. In such situations, the payphone provider should bear liability for fraud as an unfortunate cost of doing business. Neither the local nor the long distance carrier should be required to hold their customers harmless for such toll fraud liability.[6]

3. The IXC and the LEC cannot always positively identify fraud; sometimes, all they can do is detect unusual traffic patterns and alert the customer to such anomalous activity. It is the customer's responsibility to determine whether such activity is legitimate or fraudulent, and (absent grant of prearranged authority to the carrier to disable accounts which exceed specified limits) to notify the carrier as to what corrective action (if any) should be taken. However, if, contrary to Sprint's view, the carrier is required to assume responsibility for some or most of the fraud since it is in the "best position" to detect unusual traffic patterns, then the carrier should be able to terminate the apparently compromised ANI on its own authority and initiative. Under these circumstances, the carrier should not be held liable for wrongful termination of service.

---

[6]Of course, if the carrier chooses to act in such capacity for the customer (as is the case with Sprint's SprintGuard Plus service), it should be free to do so.

III. THE INDUSTRY IS CONSIDERING WAYS TO PREVENT OR MINIMIZE PAYPHONE AND CELLULAR TOLL FRAUD.

The Commission seeks comment on whether there are services available to payphone providers and to cellular customers that may reduce the risk of fraud (NPRM, paras. 31 and 34). As discussed briefly below, there are both existing and potential additional measures which can be taken to reduce payphone and cellular fraud.

A. Payphone fraud.

The Commission notes that payphone providers may use screening services (OLS and BNS) and the no-PIC option to reduce the possibility of toll fraud.[7] According to preliminary data compiled by the United and Central telephone companies, it appears that the percentage of payphone providers which subscribe to OLS and BNS services varies significantly by jurisdiction. For example, in Florida, Nevada, Oregon, and Washington, subscription rates are 100 percent. However, in other states, subscription rates for BNS are in the single digit range (including in United/Centel's Illinois and Missouri exchanges, where BNS is available at no monthly charge). Available information indicates that these blocking and screening services are working as intended.

However, it should be recognized that subscription to LEC-provided blocking and screening services will not prevent

---

[7]Sprint would point out that the efficacy of the "no-PIC" option in minimizing toll fraud is problematic unless the payphone provider also blocks 10XXX+1 calls using either its own equipment or services obtained from the LECs.

all types of payphone fraud. For example, OLS and BNS will not prevent fraud perpetrated by means of physical access to the line between the payphone and the LEC central office. A payphone provider can, however, take other steps to reduce the risk of fraud, such as blocking inbound calls (where permissible), placing the payphone in a physically secure spot (e.g., one which is well-lit and visible to the premises owner), or installing equipment which sends a special tone or announcement identifying the line as a payphone.[8]

Finally, Sprint would note that to combat international toll fraud, the industry is considering a proposal that payphones be in the 8000 and 9000 numbering scheme. If a foreign operator receives a request to bill a call to a number in this series, the operator would recognize the number as a payphone, and could transfer the call to a U.S. operator, who would then initiate the LIDB query and possibly request an alternative billing mechanism.

B. Cellular fraud.

The Commission has proposed an amendment to Part 22 of the rules to help reduce tampering with cellular equipment's ESN (electronic serial number) (see NPRM, para. 34). While this proposed rule is a good start, Sprint believes that it does not go far enough. Proposed Section 22.929 would prohibit

---

[8]Even if all of these measures are taken, and every preventive device or service works properly, it is possible that some fraud will still occur. As noted above, in these unfortunate incidents, the payphone provider should accept liability as a cost of doing business.

alteration or removal of each mobile transmitter's unique ESN, i.e., modification of the stored memory location of the ESN. However, much of the counterfeiting of cellular phones today is accomplished without changing the stored ESN. Instead, the phone transmits the contents of an alternative memory location as the "ESN," thereby bypassing the original manufactured ESN. Section 22.929 should be modified to require cellular phone design which prohibits transmission of anything other than the original factory-installed ESN.[9] The ESN should not be modifiable via the phone's data port.

Cellular carriers could help to reduce toll fraud in at least two other ways: by transmitting the information digits (the "II" digits 61, 62 and 63) which identify a call as originating from a cellular phone; and by performing pre-call verification on every cellular call. Provision of the II digits will notify the IXC that the call is from a cellular phone, and the traffic patterns can be compared to a "cellular profile";[10] and pre-call validation would detect high volumes of validation attempts, indicating possible tumbling and/or multiple users for an ESN.

---

[9]The only exception would be to allow authorized dealers to move the ESN from one phone to another for maintenance purposes. Even when this is done, there remains only one phone with the unique ESN.

[10]Sprint Communications Company is working with cellular companies to design monitoring capabilities to fit a cellular profile. As is the case for other services, when Sprint detects unusual traffic activity, it could then notify the cellular customer and take corrective action.

IV. ALTERNATIVE BILLING SERVICES-RELATED FRAUD CAN BE REDUCED THROUGH COOPERATIVE EFFORTS.

In the NPRM (paras. 35-39), the Commission seeks comment on several issues related to Alternative Billing Services ("ABS")[11] related fraud, including the relative ability of LIDB users and providers to detect fraud; whether provision of information on the origination and termination points of a call will enhance fraud detection; and assignment of liability for toll losses among LIDB providers and LIDB customers. Sprint discusses below steps various parties can take--including implementation of and adherence to clearly articulated LIDB service standards and the provision of called from/called to data--which could help to minimize ABS-related fraud.[12] These steps can help to apportion liability for ABS-related toll fraud. For example, if the LIDB provider fails to meet agreed-upon operational service standards, or mishandles the LIDB information within its control, the LIDB provider should assume liability for any resulting ABS-related fraud. Clearly

---

[11]Alternative Billing Services refer to collect calls, third number billed calls, and calling card calls. Although the Commission refers to "Line Information Database (LIDB) fraud," ABS fraud is a more accurate term, since the fraud is committed through abuse of ABS calling, not through the use of a LIDB.

[12]The LIDBs and associated administrative processes clearly can be effective tools in the industry's efforts to combat ABS-related fraud. However, the LIDB alone cannot prevent all ABS-related fraud. LIDBs cannot detect all of the many different calling patterns generated by those who would defraud telecommunications service providers (NPRM, para. 39), and sophisticated fraud perpetrators can determine at least some of the controls used to detect fraud, and then generate fraudulent calls in a manner that circumvents these controls.

defining LIDB service and operational standards and expectations (determined jointly by LIDB providers and users) is a key step in determining apportionment of liability between LIDB users and providers.

A. The LIDB Providers Should Clarify and Commit to Specific Operational Service Standards

In Sprint's view, LIDB service comprises not only validation functions, but also anti-fraud adjunct systems and investigative processes and resources. LIDB providers must commit to and implement certain minimum industry-wide LIDB service standards (to be determined based upon discussions in appropriate industry fora with their customers),[13] and should accept liability for any fraud which results from their (LIDB providers') failure to meet these standards.

Pending development of industry-wide standards, LIDB providers should define their current operational service standards. Some LIDB providers have refused to disclose, or even discuss, with Sprint Long Distance such things as the fraud trigger thresholds they employ or how these thresholds were determined. As a consequence, Sprint Long Distance, and perhaps other IXCs as well, have had to deploy many monitoring devices which may well be redundant to (and possibly

---

[13] In most cases the LIDB provider is also a LIDB user. For instance, the United telephone companies are the second largest user of their own LIDB service and a substantial user of other entities' LIDBs for purposes of validating ABS-related calling on the United network. As both a LIDB provider and as a LIDB user, United therefore has an interest in seeing the LIDB and all available fraud minimization tools utilized to the fullest extent.

inconsistent with) devices used by the LIDB providers. While Sprint fully supports the principle that all parties should employ all means at their disposal to combat fraud, it is a poor use of resources to duplicate efforts unnecessarily. Until all LIDB providers fully define the nature of the service currently being provided, Sprint Long Distance will feel compelled to continue to deploy these possibly redundant fraud detection mechanisms.

Second, LIDB providers and their customers should establish operational standards which specify the steps that the LIDB providers will take upon receipt of a fraud referral from the customer. Because it does not know how the LIDB provider will investigate and react to such referrals, Sprint Long Distance often has to restrict certain calls from its network, even though the LIDB provider has not yet deactivated the card or imposed billed number screening on the number in its database. This situation causes customer confusion and anger (directed at Sprint Long Distance) when the customer is unable to use a joint calling card to place calls on the Sprint network, but can use it on other networks.

Third, LIDB providers must design and adhere to both normal and emergency update processes which ensure that the LIDB contains the most accurate and up-to-date information possible.[14] They should react immediately to referrals from

---

[14]The FCC has already taken some steps to help ensure that these update processes are adhered to (see In the Matter

(Footnote Continued)

any party which believes fraud is occurring, and, as noted above, should develop procedures for coordinating with LIDB users once a fraud referral is received. If the LIDB provider mishandles information within its control--for example, if it receives the correct information, but fails to enter such information or to fix incorrect information in accordance with the agreed-upon standards and procedures--the LIDB provider should be liable for any fraud which results from this failure.

Fourth, once they receive "called to" and "called from" information (discussed below), the LIDB providers must implement processes to use such information to identify suspicious traffic patterns. Once such suspicious traffic patterns are detected, the LIDB provider must react quickly to them in accordance with agreed-upon standards and procedures.

Fifth, LIDB providers must explain in greater detail the specific set of factors that give rise to a particular LIDB query response so that a well-informed decision can be made on whether to pass traffic under certain response conditions. Inconsistencies in how and when updates occur between the LIDB and the LEC Customer Database, and in how and when information digits are passed to the IXCs, create additional customer and IXC confusion.

(Footnote Continued)
of Local Exchange Carrier Line Information Database, CC Docket No. 92-24, Order released August 23, 1993 ("LIDB Investigation Order"), paras. 27-34). However, these steps are insufficient because they do not apply to non LEC-owned LIDBs and do not place any obligation upon the party which is normally the closest to the data--the LEC which issued the calling card or which is associated with the billed line number.

Sixth, LIDB providers and users must work together to develop and implement future enhancements to the LIDB and adjunct fraud systems of both parties which will further improve LIDB as an anti-fraud tool.

B. Other Members of the Industry Must Also Take an Active Role in Preventing ABS Fraud.

As the Commission noted in the NPRM (para. 36), LIDB customers also have an obligation to use the LIDB in a manner which reduces the risk of toll fraud. In particular, LIDB users must validate each and every ABS call.[15] Only if such validation takes place on all such calls will the LIDB thresholds be able to track call attempts and detect excessive use that indicates possible fraudulent activity.[16] If the OSP or IXC chooses not to validate ABS calls using LIDB, then that OSP or IXC should be liable for any resulting fraud, including fraud on other carriers' networks which is due to the OSP/IXC's failure to validate.

Additionally, Sprint believes that LIDB users should pass the "called to" and "called from" numbers with the query. This information gives the LIDB provider an additional valuable tool for detecting fraud, particularly in the international arena. Provision of called to and called from information

---

[15]This includes multiple calls dialed through the "pound" key that do not require the calling card number and PIN to be entered for each successive call.

[16]The United telephone companies' LIDB uses these call volume thresholds to trigger fraud investigations and automatic deactivation. For these thresholds to be effective, all call attempts must be tracked.

will enable LIDB fraud detection systems to better track high volume use and unusual traffic patterns that may indicate fraud, e.g., the same card number being used simultaneously in multiple parts of the world.

Sprint Long Distance currently plans to pass the called to and called from numbers to the LIDB provider at no charge, on the theory that such information provides additional intelligence that is of value in detecting fraud. However, in exchange for the provision of this information, the LIDB providers' systems and processes must be modified to recognize the information and to use such information to monitor traffic to better control and prevent fraud.[17] Furthermore, because provision of called from/called to data improves the quality of LIDB service, the LIDB provider would be expected to accept a greater level of liabilty for fraud if it has access to this data.

The carrier of the call should also attempt to monitor the traffic on its network to determine if it is experiencing unusual patterns such as long duration calling or spikes from or to specific locations, because the attempts to defraud may involve data in more than one LIDB. For instance, calling cards issued by several LECs may be stolen at one time and used alternatively as part of a scheme of heavy fraudulent calling to one country. While no single LIDB will be able to

---

[17]LIDB providers should be strictly prohibited from using called to and called from data for any purpose other than preventing fraud.

see all of this fraudulent activity, the carrier may be able to see unusually heavy calling to that part of the world and to investigate whether such activity is legitimate or fraudulent.

Carriers should also work towards sharing of information gathered during the subscription process to prevent access to those who have a high potential for perpetrating fraud (e.g., customers who use the same name and different addresses to establish new service, but have previously unpaid bills with any carrier). Additionally, IXCs and LIDB providers could create system interfaces that would serve as real-time fraud information sharing mechanisms.

Finally, preventive measures should be taken by the billing carrier (e.g., calling card issuers should ensure that the card numbers and PINs are not stolen during the issuance process and should act on reports of lost or stolen cards immediately so that the LIDB can be properly updated); by payphone providers (which should take steps to create a more secure calling environment, e.g., to prevent "shoulder surfing" and "clip on" fraud); and by customers (who must be made aware of how fraud occurs and how they can help to prevent unauthorized access to their card and PIN numbers).

* * * * *

In order to minimize the risk of ABS-related fraud, Sprint recommends the following:

- LIDB providers and users must work together to determine, at a detailed level, the exact situations that create certain responses from the LIDB database, and the specific operational

service standards to which the LIDB providers must commit. At a minimum, standards for the following factors must be defined by the LIDB providers and users:

- o the extent of verification and sharing of customer information needed to prevent fraud, particularly on new service;
- o the point at which LIDB users should be notified of high risk accounts;
- o the timeframes for service order/system updates and for responses to fraud referrals;
- o the content and method of transmission for fraud referrals;
- o the extent of availability and use of called to and called from numbers;
- o all ANI "II" digits and, where available, flex ANI information; and
- o any additional expectations that could limit fraud exposure.

- LIDB providers and users must work together (perhaps through the TFPC, discussed above) to ensure that the development of new systems and the enhancements of current systems address areas that are best handled by each entity to avoid wastefully duplicative fraud detection measures. In addition, enhancements to the LIDB and all adjunct systems and processes need to address all calling patterns and call types.

- The FCC should extend the existing tariff obligations for LEC-owned LIDBs to all LIDB providers.[18] Because the

---

[18] In the LIDB Investigation Order (para. 19), the Commission required the LEC-owned LIDB providers to include in their tariff information on the frequency of database updates, the type of information included in the updates, the speed

(Footnote Continued)